### PATENT COOPERATION TREATY

REC'D 0 7 MOV 2005

WIPO

#### From the INTERNATIONAL SEARCHING AUTHORITY **PCT**

To: PHILIP R. WADSWORTH

QUALCOMM INCORPORATED 5775 MOREHOUSE DRIVE SAN DIEGO, CA 92121		WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY			
			(PCT Rule 43bis.1)		
		Date of mailing (day/month/year)	03 NOV 5002		
Applicant's or agent's file reference		FOR FURTHER	ACTION See paragraph 2 below		
030457WO	International filing date	(day/month/year)	Priority date (day/month/year)		
Thick national apparatus		:	29 October 2003 (29.10.2003)		
PCT/US04/36284 28 October 2004 (28.10 International Patent Classification (IPC) or both national classification		ation and IPC	25 000000 2000 (25 1000)		
IPC(7): H04L 9/00 and US C1.: 713/176 Applicant					
QUALCOMM INCORPORATED					
QUALCONNI INCONT CITATIBE					
1. This opinion contains indications re	ating to the following ite	ms:	•		
Box No. I Basis of th	Basis of the opinion				
Box No. II Priority	·				
Box No. III Non-estab	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability				
1 1 2	Lack of unity of invention				
Box No. V Reasoned applicabili	Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement				
Box No. VI Certain do	Certain documents cited				
Box No. VII Certain de	Certain defects in the international application				
Box No. VIII Certain of	servations on the interna	tional application			
2. FURTHER ACTION					
If a demand for international preli	ing Authorny (IFEA)	en IPEA has notified 1	be considered to be a written opinion of the s not apply where the applicant chooses an the International Bureau under Rule 66.1bis(b) dered.		
iPEA a written reply together, who of Form PCT/ISA/220 or before the	ere appropriate, with and e expiration of 22 month	vritten opinion of the endments, before the e s from the priority date	IPEA, the applicant is invited to submit to the expiration of 3 months from the date of mailing be, whichever expires later.		
For further options, see Form PCT	/ISA/220.				
3. For further details, see notes to Fo					
Name and mailing address of the ISA/ US Date of com		npletion of this opinior			
		2005 (17.10.2005)	Joseph Pan		
P.O. Box 1450 Alexandria, Virginia 22313-145			Telephone No. 571-272-5987		
Facsimile No. (571) 273-8300 Form PCT/ISA/237 (cover sheet) (April					

# WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

International application No.
PCT/US04/36284

Box No. I Basis of this opini	on
1. With regard to the language, the	his opinion has been established on the basis of:
the international appli	cation in the language in which it was filed
international search (Ru	
2. With regard to any nucleotide invention, this opinion has bee	and/or amino acid sequence disclosed in the international application and necessary to the claimed n established on the basis of:
a. type of material	
a sequence listing	
table(s) related to	the sequence listing
b. format of material	
on paper	
in electronic form	n
c. time of filing/furnishin	g
contained in the	international application as filed.
filed together w	ith the international application in electronic form.
	quently to this Authority for the purposes of search.
	•
9 1 1 11	e that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed ired statements that the information in the subsequent or additional copies is identical to that in the does not go beyond the application as filed, as appropriate, were furnished.
4. Additional comments:	

Form PCT/ISA/237(Box No. I) (April 2005)

## WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

Form PCT/ISA/237 (Box No. V) (April 2005)

International application No. PCT/US04/36284

INTERNATIONAL CENTRE		11 /			
Box No. V Reasoned statement under Rule 43 bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement					
1. Statement					
	Claima 1 45		YES		
Novelty (N)			NO		
	Claims NOTE				
Inventive step (IS)	Claims NONE		YES		
myentive step (12)					
Industrial applicability (IA)					
1.	Claims NONE		NO		
2. Citations and explanations:					
Please See Continuation Sheet					
		·			
		,			

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY International application No. PCT/US04/36284

V. 2. Citations and Explanations:  Claims 1-45 lack inventive step under PCT effice 33(3) as being obvious over Draws (U.S. Patent No. 6,477,645) in view of Bari et al. (U.S. Pub. No. 2002/002309).  Draws discloses referring to PGS. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking public key is shown. System 100 includes remote platform 105, user platform 110, including checks in a system lacking public key is shown. System 100 includes remote platform 105, user platform 110, including checks in a system lacking public key is shown. System 100 includes remote platform 105, user platform 110, including checks in a system lack public key is shown. System 100 includes remote platform 105, user platform 110, coupled to user platform 100 includes a system 120 of user platform 100 is capable of receiving input, such as credential transformation view 145, from authorizing entity 150 or origination 100, which includes credential subset transformation view 145, from authorizing entity 150 origination 100, which includes credential subset 165 from authorizing entity 150.  Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 100. Remote platform 105 is not immediate to any particular type of device and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, Such as a caliphone, or a television or endo transmitter or computer, a server or a mainframe, or a communication device, Such as a caliphone, or a television or endo transmitter or transcelver. Those skilled in the art will recorptize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present fivention transmitted from remote platform 50 to user platform 110. In one embodiment of the incommitted in the present invention is equally applicable to the transmitted information transmitted from remote platform 40 to 10 to use	In case the space in any of the preceding boxes is not sufficient.
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FIG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential fransformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential fransformation value 135, information transformation value 140, or credential subset transformation value 145, from authorizing entity 150 for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmitsed information, such as a digital certificate that normall	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FIG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential fransformation user platform 140, or credential subset transformation value 145, from authorizing entity 150 value 135, information transformation value 140, or credential subset transformation value 145, from authorizing entity 150 for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110 in one embodiment of the authority and integrity of information received at user platform 110, so it is not limited in the present invention in transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, such as a digital s	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FIG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving information 145 and for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 105. In the present invention to user platform 105. The present invention in transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, such as a digital signature in combination with other information, such as a digital certific	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation value 135, information transformation value 140, or credential subset transformation value 145, from authorizing entity 150 value 135, information system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmitssion of information, such as a digital certificate that norma	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 105 is capable of receiving information 155 and for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal ransceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, such as a digital signature or digital	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 105 is capable of receiving information 155 and for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal ransceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, such as a digital signature or digital	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 105 is capable of receiving information 155 and for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal ransceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, such as a digital signature or digital	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 105 is capable of receiving information 155 and for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal ransceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, such as a digital signature or digital	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 105 is capable of receiving information 155 and for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal ransceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, such as a digital signature or digital	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 105 is capable of receiving information 155 and for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal ransceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, such as a digital signature or digital	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 105 is capable of receiving information 155 and for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal ransceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, such as a digital signature or digital	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 105 is capable of receiving information 155 and for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal ransceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, such as a digital signature or digital	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation value 135, information transformation value 140, or credential subset transformation value 145, from authorizing entity 150 value 135, information system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105. In the server or a mainframe, or a communication device, Such as a cell phone, or a television or racio transmitter or transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmitssion of information, such as a digital certificate that no	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation value 135, information transformation value 140, or credential subset transformation value 145, from authorizing entity 150 value 135, information system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105. In the server or a mainframe, or a communication device, Such as a cell phone, or a television or racio transmitter or transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmitssion of information, such as a digital certificate that no	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 105 is capable of receiving information 155 and for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal ransceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, such as a digital signature or digital	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 105 is capable of receiving information 155 and for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal ransceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, such as a digital signature or digital	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation value 135, information transformation value 140, or credential subset transformation value 145, from authorizing entity 150 value 135, information system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105. In the server or a mainframe, or a communication device, Such as a cell phone, or a television or racio transmitter or transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmitssion of information, such as a digital certificate that no	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to transformation value 145, comparison system 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation value 135, information transformation value 140, or credential subset transformation value 145, from authorizing entity 150 for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, Such as a ceil phone, or a television or racio transmitter or transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the transmission of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will reco	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to transformation value 145, comparison system 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation value 135, information transformation value 140, or credential subset transformation value 145, from authorizing entity 150 for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, Such as a ceil phone, or a television or racio transmitter or transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the transmission of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will reco	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to transformation value 145, comparison system 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation value 135, information transformation value 140, or credential subset transformation value 145, from authorizing entity 150 for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, Such as a ceil phone, or a television or racio transmitter or transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the transmission of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will reco	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to transformation value 145, comparison system 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation value 135, information transformation value 140, or credential subset transformation value 145, from authorizing entity 150 for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, Such as a ceil phone, or a television or racio transmitter or transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the transmission of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will reco	
Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Barl et al. (U.S. Pub. No. 2002/0023059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to transformation value 145, comparison system 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation value 135, information transformation value 140, or credential subset transformation value 145, from authorizing entity 150 for input into comparison system 120 of user platform 110. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, Such as a ceil phone, or a television or racio transmitter or transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the transmission of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will reco	V. 2. Citations and Explanations:
Bari et al. (U.S. Pub. No. 2002/0029059).  Drews discloses referring to FiG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including checks in a system lacking a public key is shown. System 120, and display system 122. Remote platform 105 is coupled to transformation value generator 115, comparison system 120 and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation value 145, from authorizing entity 150 for input into comparison system 120 of user platform 110. Remote platform 105 is capable of receiving information 155 and credential 160, which includes credential subset 155 from authorizing entity 150.  Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, Such as a cell phone, or a television or radio transmitter or transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmission of information, such as a application software or data.  Credential 160, in one embodiment, contains authority information, such as a digital signature or digital signature in combination with other information, such as a digital	
Drews discloses referring to FIG. 1, a block diagram of one embodiment of system 105, user platform 110, including checks in a system lacking a public key is shown. System 120, and display system 122. Remote platform 105 is coupled to transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation value 135, information transformation value 140, or credential subset transformation value 145, from authorizing entity 150 for input into comparison system 120 of user platform 110. Remote platform 105 is capable of receiving information 155 and credential 160, which includes credential subset 185 from authorizing entity 150.  Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, Such as a cell phone, or a television or radio transmitter or transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmitted information such as application software or data.  Credential 160, in one embodiment, contains authority information, such as a digital signature or digital signature in combination with other information, such as a digital certificate that normally accompanies  Credential 160, in one embodiment, contains authority	Claims 1-45 lack inventive step under PC1 article 35(3) as being obvious svor Brons (1-45).
checks in a system lacking a public key is shown. System 100 indicates that the present invention value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation value 135, information transformation value 140, or credential subset transformation value 145, from authorizing entity 150 for input into comparison system 120 of user platform 110. Remote platform 105 is capable of receiving information 155 and credential 160, which includes credential subset 165 from authorizing entity 150. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, Such as a cell phone, or a television or radio transmitter or transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmission of information such as application software or data.  Credential 160, in one embodiment, contains authority information, such as a digital signature or digital signature in combination with other information, such as a digital certificate that normally accompanies transmitted information. The authority information, without a public key that designates the authority of the credential. However, a credential which includes a digital on user platform 10, is insufficie	
transformation value generator 115, comparison system 120, and user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation value 145, from authorizing entity 150 value 135, information transformation value 140, or credential subset transformation 105 is capable of receiving information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110. The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmitsion of information such as application software or data.  Credential 160, in one embodiment, contains authority information, such as a digital signature or digital signature in combination with other information, such as a digital certificate that normally accompanies transmitted information. The authority information, without a public key that designates the authority of the credential. However, a credential which includes a	checks in a system lacking a public key is snown. System 100 and display outton 122. Remote platform 105 is coupled to
value 135, information transformation value 140, or credential subset transpart of input into comparison system 120 of user platform 110. Remote platform 105 is capable of receiving information 155 and credential 160, which includes credential subset 165 from authorizing entity 150.  Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, Such as a ceil phone, or a television or radio transmitter or computer, a server or a mainframe, or a communication device, Such as a ceil phone, or a television or radio transmitter or computer, a server or a mainframe, or a communication device, Such as a ceil phone, or a television or radio transmitter or computer, a server or a mainframe, or a communication device, Such as a ceil phone, or a television or radio transmitter or computer, a server or a mainframe, or a communication device, Such as a ceil phone, or a television or radio transmitted information 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the present invention as remote platform 105 to user platform 110. In one embodiment of the invention, the type of information remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to information with other information, such as a application software or data.  Credential 160, in one embodiment, contains authority information, such as a digital signature or digital signature in combination with other information, such as a digital certificate that normally accompanies transmitted information. The authority information, without a public key that designates the authority of the credential. However,	transformation value generator 115, comparison system 120, and display system input, such as credential transformation
for input into comparison system 120 of user platform 110. Reinfote platform 150. credential 160, which includes credential subset 165 from authorizing entity 150. Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, Such as a cell phone, or a television or radio transmitter or transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmission of information such as application software or data.  Credential 160, in one embodiment, contains authority information, such as a digital signature or digital signature in combination with other information, such as a digital certificate that normally accompanies transmitted information. The authority information, without a public key that designates the authorized source of the credential's digital signature installed on user platform 110, is insufficient to check the authority of the credential. However, a credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential.  User platform 110 is provided for the purpose of receiving transmitted information such as information 155, credential 160, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, or information 155 and credential 160 from remote platform	user platform 110 by communication triangle 125. Soon post of the platform 110 by communication triangle 145, from authorizing entity 150 years 135, information transformation value 145, from authorizing entity 150
credential 160, which includes credential subset 105 into authorizing entitling information 155 and credential 160 to user Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmission of information such as application software or data.  Credential 160, in one embodiment, contains authority information, such as a digital signature or digital signature in combination with other information, such as a digital ertificate that normally accompanies transmitted information. The authority information, without a public key that designates the authorized source of the credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential.  User platform 110 is provided for the purpose of receiving transmitted information such as information 155, credential 160, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, commands, or data staged on remote platform 105, and can be a computer, such as a personal computer, a ser	5 - 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
platform 110. Remote platform 105 is not limited to any particular type of the too or a television or radio transmitter or computer, a server or a mainframe, or a communication device, Such as a cell phone, or a television or radio transmitter or transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to information of information such as application software or data.  Credential 160, in one embodiment, contains authority information, such as a digital signature or digital signature in combination with other information, such as a digital certificate that normally accompanies transmitted information. The authority information, without a public key that designates the authorized source of the credential's digital signature installed on user platform 110, is insufficient to check the authority of the credential. However, a credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential.  User platform 110 is provided for the purpose of receiving transmitted information such as information 155, credential 160, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, commands, or data staged on remote platform 105, and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like remote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the	credential 160, which includes credential subset 165 floor authorizing entering 160, which includes credential 160 to user
computer, a server or a mainframe, of a communication device, state as a complete of transmitting information to user platform 110 transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the present invention as a platform 110 information information information information information information information information information security information, such as a digital signature or digital signature in combination with other information, such as a digital certificate that normally accompanies transmitted information. The authority information, without a public key that designates the authorized source of the credential signature installed on user platform 110, is insufficient to check the authority of the credential. However, a credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential.  User platform 110 is provided for the purpose of receiving transmitted information such as information 155, credential 160, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, commands, or data staged on remote platform 105, and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like remote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the art will recognize that any device capable of receiving information from remote platform 105 can be used in the present invention.	Remote platform 105 is capable, in one embodiment, of staying and transmitting information to the staying and
transceiver. Those skilled in the art will recognize that any device capable of standard can function as remote platform 105.  The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the present invention ensures the authority and integrity of information 110. In one embodiment of the invention, the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmission of information such as application software or data.  Credential 160, in one embodiment, contains authority information, such as a digital signature or digital signature in combination with other information, such as a digital certificate that normally accompanies transmitted information. The authority information, without a public key that designates the authorized source of the transmitted information. The authority information 110, is insufficient to check the authority of the credential signature installed on user platform 110, is insufficient to check the authority of the credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential.  User platform 110 is provided for the purpose of receiving transmitted information such as information 155, credential 160, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, commands, or data staged on remote platform 105, and can be a computer, such as a personal computer, a server or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like remote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the art will recognize that any device capable of receiving information from remote platform 105 can be used in the	platform 110. Remote platform 100 is not limited to drift position at the platform 110. Remote platform 100 is not limited to drift position at the platform 110. Remote platform 110 is not limited to drift position at the platform 110. Remote platform 110 is not limited to drift position at the platform 110. Remote platform 100 is not limited to drift position at the platform 110. Remote platform 100 is not limited to drift position at the platform 110. Remote platform 110 is not limited to drift position at the platform 110. Remote platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position at the platform 110 is not limited to drift position 110 is not limited to drif
can function as remote platform 105. The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the present invention ensures the authority and integrity of information received at user platform 110. In one embodiment of the invention, the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmission of information such as application software or data.  Credential 160, in one embodiment, contains authority information, such as a digital signature or digital signature in combination with other information, such as a digital certificate that normally accompanies transmitted information. The authority information, without a public key that designates the authorized source of the credential's digital signature installed on user platform 110, is insufficient to check the authority of the credential. However, a credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential.  User platform 110 is provided for the purpose of receiving transmitted information such as information 155, credential 160, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, or information device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like remote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the art will recognize that any device capable of receiving information from remote platform 105 can be used in the prese	transceiver. Those skilled in the art will recognize that any device capable of transferring
the type of information transmitted from remote platform 105 to describe that the present invention is equally applicable to information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmission of information such as application software or data.  Credential 160, in one embodiment, contains authority information, such as a digital signature or digital signature in combination with other information, such as a digital certificate that normally accompanies transmitted information. The authority information, without a public key that designates the authorized source of the credential's digital signature installed on user platform 110, is insufficient to check the authority of the credential. However, a credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential.  User platform 110 is provided for the purpose of receiving transmitted information such as information 155, credential 160, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, commands, or data staged on remote platform 105, and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like remote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the art will recognize that any device capable of receiving information from remote platform 105 can be used in the present invention. (see column 2, lines 9-65 of Drews).	can function as remote platform 105.
information 155 is a boot image, but those skilled iff the art will ready lize that the process that the transmission of information such as application software or data.  Credential 160, in one embodiment, contains authority information, such as a digital signature or digital signature in combination with other information, such as a digital certificate that normally accompanies transmitted information. The authority information, without a public key that designates the authorized source of the transmitted information to check the authority of the credential. However, a credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential.  User platform 110 is provided for the purpose of receiving transmitted information such as information 155, credential 160, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, commands, or data staged on remote platform 105, and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like remote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the art will recognize that any device capable of receiving information from remote platform 105 can be used in the present invention. (see column 2, lines 9-65 of Drews).	The present invention ensures the authority and integrity of information reserved as a property of the invention,
the transmission of information such as application software of data.  Credential 160, in one embodiment, contains authority information, such as a digital signature or digital signature in combination with other information, such as a digital certificate that normally accompanies transmitted information. The authority information, without a public key that designates the authority of the credential. However, a credential's digital signature installed on user platform 110, is insufficient to check the authority of the credential. However, a credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential.  User platform 110 is provided for the purpose of receiving transmitted information such as information 155, credential 160, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, or commands, or data staged on remote platform 105, and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like remote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the art will recognize that any device capable of receiving information from remote platform 105 can be used in the present invention. (see column 2, lines 9-65 of Drews).	information 155 is a hoot image, but those skilled in the dit will recognize that the pro-
Credential 160, in one embodiment, contains authority information, such as a digital combination with other information, such as a digital certificate that normally accompanies transmitted information. The authority information, without a public key that designates the authority of the credential. However, a credential's digital signature installed on user platform 110, is insufficient to check the authority of the credential. However, a credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential.  User platform 110 is provided for the purpose of receiving transmitted information such as information 155, credential 160, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, or adata staged on remote platform 105, and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like remote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the art will recognize that any device capable of receiving information from remote platform 105 can be used in the present invention. (see column 2, lines 9-65 of Drews).	
transmitted information. The authority information, without a public key that designate authority of the credential. However, a credential's digital signature installed on user platform 110, is insufficient to check the authority of the credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential.  User platform 110 is provided for the purpose of receiving transmitted information such as information 155, credential 160, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, or information 155 and credential 160 from remote platform 105, and can be a computer, such as a personal computer, a server or a commands, or data staged on remote platform 105, and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like remote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the art will recognize that any device capable of receiving information from remote platform 105 can be used in the present invention. (see column 2, lines 9-65 of Drews).	Credential 160, in one embodiment, contains authority information, such as a digital agreement of
credential's digital signature installed on user platform 110, is installed in to credential can be used to check the integrity of the credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential.  User platform 110 is provided for the purpose of receiving transmitted information such as information 155, credential 160, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, or information 155 and credential 160 from remote platform 105, and can be a computer, such as a personal computer, a server or a commands, or data staged on remote platform 105, and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like remote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the art will recognize that any device capable of receiving information from remote platform 105 can be used in the present invention. (see column 2, lines 9-65 of Drews).	combination with other information, such as a digital certificate that horning description without a public key that designates the authorized source of the
credential which includes a digital signature that covers the rest of the detectation of the credential credential.  User platform 110 is provided for the purpose of receiving transmitted information such as information 155, credential 160, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, or information 155 and credential 160 from remote platform 105, and can be a computer, such as a personal computer, a server or a commands, or data staged on remote platform 105, and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like remote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the art will recognize that any device capable of receiving information from remote platform 105 can be used in the present invention. (see column 2, lines 9-65 of Drews).	transmitted information. The authority meant and transmitted information. The authority of the credential. However, a credential's digital signature installed on user platform 110, is insufficient to check the authority of the credential.
credential. User platform 110 is provided for the purpose of receiving transmitted information such as information 155, credential 160, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, or information 155 and credential 160 from remote platform 105, user platform 105, and can be a computer, such as a personal computer, a server or a commands, or data staged on remote platform 105, and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like memote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the art will recognize that any device capable of receiving information from remote platform 105 can be used in the present invention. (see column 2, lines 9-65 of Drews).	credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the
or information 155 and credential 160 from remote platform 105. Ose platform 105 as a personal computer, a server or a commands, or data staged on remote platform 105, and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like remote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the art will recognize that any device capable of receiving information from remote platform 105 can be used in the present invention. (see column 2, lines 9-65 of Drews).	credential. credential formation such as information 155, credential 160,
commands, or data staged on remote platform 105, and can be a computer, such as a pager. Like mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like mainframe, or a communication that any device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like remote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the art will recognize that any device capable of receiving information from remote platform 105 can be used in the present invention. (see column 2, lines 9-65 of Drews).	User platform 110 is provided for the purpose of receiving a a striked anishment 110 is the target device for software,
mainframe, or a communication device, such as a pager, a cert priorie, or a total visite, and those skilled in the art will remote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the art will remote platform 105 can be used in the present invention. (see column 2, lines 9-65 of Drews).	commands, or data staged on remote platform 105, and can be a computer, such as a personal computer, a server or a
remote platform 105, user platform 110 is not limited to any particular type of government of used in the present invention. recognize that any device capable of receiving information from remote platform 105 can be used in the present invention. (see column 2, lines 9-65 of Drews).	mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like
recognize that any device capable of receiving information from remote platform. (see column 2, lines 9-65 of Drews).	remote platform 105, user platform 110 is not limited to any particular type of device, and those stated in the different invention.
(see column 2, lines 9-05 of Disws).  Transferred to provide a variable length amount of digital data into a more concise form.	recognize that any device capable of receiving information from remote platform 755
TRAISIDITIANON VAIDE DELICITION FOR THE MAIN AND	(see column 2, lines 9-00 of Diews).  Transformation value generator 115 is provided to convert a variable length amount of digital data into a more concise form.
Transformation value generator 115 is provided to convert a variable length amount of displacement of the invention, generator 115 is a hash function. A hash function accepts any length input and In one embodiment of the invention, generator 115 is a hash function. A hash function accepts any length input and In one embodiment of the invention, generator 115 is a hash function.	In one embodiment of the invention, generator 115 is a hash function. A hash function accepts any length input and
In one embodiment of the invention, generator 115 is a hash function. A hash function are known in the art and those skilled in the art will recognize that a hash Form PCT/ISA/237 (Supplemental Box) (April 2005)	generates a fixed length output. Hash full cloths are known in the circuit who should be seen a second to the circuit which is a circuit when the circuit which is a circuit when the circuit which is a circuit when the circuit when the circuit which is a circuit when the circuit which is a circuit when the circuit which is a circuit when the cir

Form PCT/ISA/237 (Supplemental Box) (April 2005)

International application No. PCT/US04/36284

### WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

function suitable for use in embodiments of the present invention is one that is relatively easy to compute, one-way, and collision-free. (see column 3, lines 15-23 of Drews).

In one embodiment, authorizing entity 150 supplies information transformation value 140, computed from information 155, to user 130. The transformation value is computed such that all parts of the information contribute to the transformation value in a way that is one-way and collision-free. In one embodiment, user platform 110 receives information transformation value 140 from user 130. Comparison system 120 compares the received information transformation value 140 with the output of transformation value generator 115, which generates a transformation value of information 155 supplied by remote platform 105. A match authenticates information 155 by ensuring the integrity and the authority of information 155. (see column 4, lines 24-37 of Drews).

Drews discloses the claimed subject matter. However, Drews does not specifically mention using the master credential in generating the application credential. On the other hand, Bari et al. disclose a system for registering, storing and managing personal data for use over a network, wherein the master credential is utilized (see paragraph [0046], lines 10-19 of Bari et al.). It would have been obvious to a person of ordinary skill in the art at the time the invention to utilize the master credential in generating the application credential. The ordinary skilled person would have been motivated to have applied the teaching of Bari et al. into method of Drew to utilize the master credential, because once a user is registered, the inventive system recognizes and authenticates the Master Authentication Credential, which then unlocks the personalized vault containing Authentication Master Credential for third party Web Sites and the User Profile (see paragraph [0036], lines 19-23 of Bari et al.).

Claims 1-45 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.